Analysis of Denial-of-Service attacks on Wireless Sensor Networks Using Simulation

[1]Doddapaneni.krishna Chaitanya, [2]Ghosh.Arindam

Middlesex University

Abstract

Evaluation of Wireless Sensor Networks (WSN) for performance evaluation is a popular research area and a wealth of literature exists in this area. Denial-of-Service (DoS) attacks are recognized as one of the most serious threats due to the resources constrained property in WSN. The Zigbee model provided in OPNET 16 is suitable for modelling WSNs. This paper presents an evaluation of the impact of DoS attacks on the performances of Wireless Sensor Networks by using the OPNET modeller. Numerical results, discussions and comparisons are provided for various simulation scenarios. The results can be of great help for optimisation studies in WSN environments under DoS attacks as well as understanding the severity and critical nodes within the WSN. The effects of DoS attacks on the performance of WSNs are considered to critically analyse these issues.

Keywords: Wireless Sensor Network (WSN), Denial-of-Service (DoS), Zigbee nodes, OPNET 16.0, IEEE 802.15, MAC protocol.

I.INTRODUCTION

With the recent advances in modern communication systems**,** wireless networks are expected to provide communication with confidentiality, data integrity, and availability of service to the user. Confidentiality of data can simply be explained as prevention of the untrusted third party from accessing the secure data. Data integrity ensures that replay attacks are prevented and the data is not modified and availability ensures that legitimate users can access services, data and network resources when requested. As wireless sensor networks continue to grow due to the fact that they are potentially low cost and effective (providing solutions to a number of real world challenges), the need for effective security mechanisms also grow.

Most of the WSN's routing protocols are easy and straightforward because of this reason they are vulnerable to attacks. The Denial of Service attack is considered particularly as it targets the energy efficient protocols that are unique to wireless sensor networks. So we start by considering such characteristics of the network and giving their impact on the security of the network. By preventing a single device from sending traffic or by preventing the communication between the network, DoS attacks target availability of services to the users [1]. In this paper we present a survey of attacks on WSN, discuss about the various DoS attacks, and the impact of DoS on the performance of the system. The simulation results show that the impact of DoS attacks on performance of WSN can be more severe, if carried out on coordinator or router, instead of just targeting the end devices. The paper is organised as follows. In section II, we present the characteristics of Wireless Sensor Networks. Section III gives a review of attacks on WSN. Denial of Service attacks in detail are explained in section IV, followed by the proposed simulation methodology in section V, section VI gives evaluation of scenario and in section VII results are shown and conclusions about impact on DoS attacks on WSN are drawn.

II.WIRELESS SENSOR NETWORK CHARACTERISTICS

A sensor network is a special type of network. The unique characteristics of Wireless Sensor Networks separate them from the legacy communication networks. Nodes of wireless sensors can be considered as small computers, very basic in terms of interfaces and the components involved. They usually consist of a limited processing capability and memory, sensors, a radio transceiver as a communication device and a limited power source such as a battery. The characteristics include, power they can store, node failures, their ability to cope, node mobility, heterogeneity and scalability of nodes and ability to cope under harsh environmental conditions. These basic characteristics of a WSN make them vulnerable to Denial of Service attacks [3].

Difficulties encountered to secure the wireless medium are the main disadvantage for all wireless devices. The network can be jammed, unauthentic data can be transmitted and/or: traffic can be overheard by any adversary in the radio range. Physical tampering of sensors and their destruction in case they are deployed in unsecured areas is also possible. Because of the vulnerable structure of WSNs and the nature of DoS attacks it may be difficult to distinguish between an attack and a network failure.

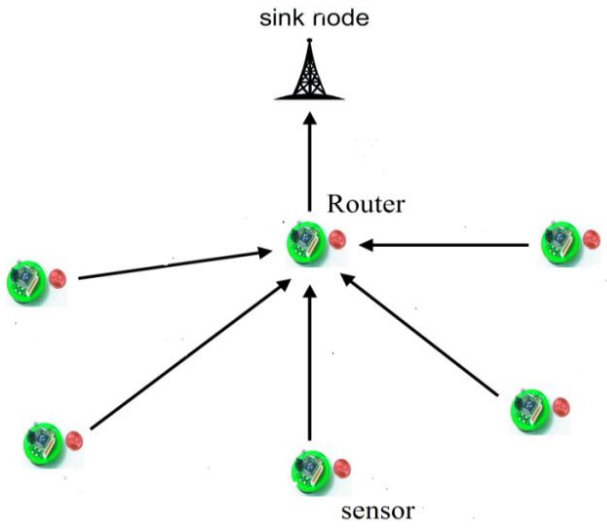

Figure 1. Simple network of WSN.

III. ATTACKS

In this section of the paper, different types of attacks have been discussed. First, attacks have been categorized as an invasive i.e. (persistent) or non-invasive i.e. (non-persistent). The Invasive attacks are usually considered more often in the literature such as [2] and they are better known attacks than the non-invasive ones. Few of the well-known Invasive attacks have been discussed in the section below, together with non-invasive attacks with the side channel attacks based on frequency, timing and power.

Attacks on sensor network routing

Most of the WSN's routing protocols are easy and straightforward. Because of this reason they are vulnerable to attacks. There are different types of network layer attacks in WSNs which can be categorised as following:

a) False routing Information, Spoofed, Altered, or replayed routing information,

b) Selective forwarding,

c) Sinkhole attacks,

d) Sybil attacks,

e) Wormholes.

In the following part of this section, the difference between attacks that strive to control the user data and attacks that attempt to influence the core routing topology are considered in details..

a) False routing Information, Spoofed, altered, or replayed routing information

In this kind of attacks, the primary focus is on the routing protocol. In the routing protocols, the main thing to be dealt is with the routing information. Therefore, by just changing the routing information of the routing protocols through malicious code, it is possible to change the complete routing structure of the Wireless Sensor Network. This can be done in a number of ways for example by replaying routing information, by shortening or extending the source routes, by spoofing bogus error messages, by altering routing loops, or by increasing the end to end delay. [2]

b) Selective forwarding

One of the fundamental principles of WSN's is that, it works on the concept to *"Multihop"*. "*Multihop*" means that the sensor node receiving the message will forward the received message to the next node in line. However, unfortunately, it is not the case in "Selective Forwarding" attacks. In "*Selective Forwarding*" the attacker attacks on one of the nodes and infects it with a malicious code which in turn acts just like any other normal node in the WSN but instead of forwarding the node in the path to the next node, it just drops those packets which make them act like a failed node [2].

Such behaviour would cause problems for the WSN considered. When this sort of situations arises the active nodes in the WSN may start to think that since the infected node is dropping all the packets, it might not be a valid node to opt to reach the desired destination. In order to cope up with these situations the attacker might pass or carry one or two of the packets forward to the next node in line to make sure nobody comes to know about the misconduct which is called "Selective Forwarding" [2].

This practice is best in "Selective Forwarding" when the attack is conducted explicitly [2]. Thus, it is believed that an attacker introducing a "Selective Forwarding" attack will likely follow the path of least resistance and attempt to include itself on the actual path of the data flow.

c) Sinkhole attacks

When Sinkhole attacks are considered, the attacker's main aim is to tempt all the nodes in close proximity constructing a figurative sinkhole. For example once the main coordinator is attacked with sinkhole all of the other nodes will also fall into the sinkhole following the main coordinator as the parent node at the centre [2].

Sinkhole attacks naturally works by assembling the attacking node to appear like an ideal node particularly targeting the neighbouring nodes. For example, an attacker could spoof or replay an advertisement for an extremely high-quality route to a base station. Then some of the protocols might try to conduct reliability and delay tests just to authenticate and confirm that the routes are valid by sending acknowledgements to the other end. The main problem arises when the laptop class attackers attacks with high quality and powerful devices within a single hop only. Therefore, due to these laptop class attacker's powerful sources and high-quality routes, it is possible that all the adjacent nodes in the area pass on the data packets through the attacker itself and also broadcasts this attractiveness to all its adjacent nodes in the vicinity. In effect, of this scenario the attacker builds a huge area of control, drawing the attention of all the traffic intended for a base station from nodes multi-hops away from the actual attacked node [2].

d) The Sybil attack

In this kind of attacks the, attacker infects a single node in the WSN network with a malevolent code masked with multiple identities. Then this single node operates as a major setback for the entire sensor network which immensely decreases the efficiency of the fault-tolerance schemes such as multipath routing, topology maintenance, disparity and distributed storage or routes which are supposed to be used by disjoint nodes but in reality could be used by only the attacker with multiple identities.

For example in this kind of attacks, it can also be proved to be of great danger to geographical routing protocols in WSN's [2]. For geographical; routing protocols, the position of the node is used in routing. These protocols involve nodes to trade and coordinate information repeatedly with each other and to their adjacent nodes to resourcefully send data packets to other destinations. Therefore, it is acceptable to have a single set of coordinates from its adjacent nodes, but on the contrary, in the Sybil Attack an attacker can be in multiple paces at the same time.

e) Wormholes

In the wormhole attacks, a malevolent node excavates the messages it receives at one end of the network over a separate low-latency channel. Then it repeats messages at a different point in the sensor network. For example, when a source node is passing on data to a destination node then there can be a malicious node in between them which selectively forwards the data packets. The wormhole attacks usually engage two different and far-away malevolent nodes conspire to minimize their remoteness from each other by replaying packets next to an out-of-reach channel which is only available to the attacker [2].

For better understanding an example can be given. In wormholes attacks the most vital thing is that, it creates a node at one end of the wormhole which then broadcasts high quality connection to the base station and another node at the other end, receiving the data packets. This happens whenever there are two conspiring nodes at a distance from the base station [2]. This Behaviour creates *routing race conditions.* As an example for the *routing race conditions* an action can be taken considering a part of the message which is being sent. Afterwards the rest of the message can be completely discarded without even being considered which the case in "Multi-hop" routing.

IV. DENIAL OF SERVICE ATTACKS:

A Denial of service attack is an explicit attempt to prevent the legitimate user of a service or data. The common method of attack involves overloading the target system with requests, such that it cannot respond to legitimate traffic. As a result, it makes the system or service unavailable for the user. The basic types of attack are: consumption of bandwidth or consumption of processor time, obstructing the communication between two machines, disruption of service to a specific system or person, disruption of routing information, disruption of physical components etc. If the sensor network encounters DoS attacks, the attack gradually reduces the functionality as well as the overall performance of the wireless sensor network. Projected use of sensor networks in sensitive and critical applications makes the prospect of DoS attacks even more alarming.

Table: Denial of Service attacks and defences to combat at different protocol layers

Protocol layer	Attacks	Defences
Physical	*Jamming*	*Sleep*
	Node destruction	*Hide nodes or tamper proof packaging*
MAC (Medium access control)	*Denial of sleep*	*Sleep, authentication and anti-replay*
Network	*Spoofing, replaying*	*Authentication, anti-replay*
	Hello floods	*Geographic routing*
	Homing	*Header encryption*
Transport	*SYN flood*	*SYN cookies*
	De synchronization attack	*Packet authentication*
Application	*Path based DoS*	*Authentication and antireplay protection.*
	Reprogramming attacks	

Mode of attack:

The three basic types of attack are:

a. Consumption of limited or scares resources(network bandwidth, memory)
b. Alteration or destruction of configuration information.
c. Physical destruction of network components.

The DoS attacks are certainly not a new phenomenon. There are standard techniques used to cope up from common DoS techniques. Some of the major types of DoS attacks are described below.

The devices which can partially or entirely disrupt a nodes signal by increasing the power spectral density are jammers. Parameters such as signal strength, location and type of jammer have great influence on the performance of the network. Another physical layer attacks include node tampering. It is not very easy to completely prevent destruction of nodes; however camouflaging and redundant nodes can mitigate this threat [4]

Denial of sleep attack causes the transmitter to remain awake for long intervals where it was not supposed to. The radio receiver consumes a lot of energy on a mote and an attack will drain as much energy so as to bring down the wireless network. Packet authentication can prevent this

attack. Continuously resetting the sleep timers, link layer authentication and anti-replay support can protect from denial of sleep attack.

Routing disruptions can lean to DoS attacks in multihop sensor networks. They include spoofing, replaying etc. Antireplay and authentication of link layer can prevent such attacks effectively. Hello messages are broadcasted by some nodes to announce themselves to their neighbours. So a node receiving such a message assumes that it is within the sender's radio range. However, sometimes a laptop class attacker broadcasting routing information with higher transmission power could convince other nodes in the network that the attacker is its neighbour. Protocols depending on localized information exchange between neighbouring nodes for flow control are affected by Hello flood attack.

The most commonly used DoS attacks is a SYN flood attack. It uses the TCP handshake mechanism. In network communication, the client sends a SYN packet; the server then returns a SYN and ACK. Then the server expects an ACK from the client. The server hence leaves the socket open and waits for the client to send the ACK packet to complete the three part handshake. Taking this as an advantage, a SYN flood attack sends thousands of SYN packets with spoofed source address. This causes the server with no resources and may malfunction badly or even crash if the operating system functions are starved of resources. SYN cookies provide protection against SYN flood as they eliminate the resources allocated on the target host. In a de-synchronization attack, an active connection is interrupted by an attacker by transmitting forged packets with control flags to desynchronize the endpoints so they retransmit the data. To overcome such attack, full packet authentication could be used [8].

In a path based DoS attack, an attacker overwhelms the sensor nodes a long distance away by injecting spurious packets or replayed packets that floods a multi hop end to end communication path. This attack consumes network bandwidth and also drains the energy of node. Combining packet authentication and antireplay can prevent from path based DoS attack.

DoS attacks in Wireless Sensor Networks can be represented in OPNET. The main aim of the paper is intended for the modelling of DoS attacks in WSN and the simulation. Section V gives an overview of the modelled WSN, simulation tool used and the standard scenario considered.

V. THE PROPOSED SIMULATION METHODOLOGY

The simulation model implements MAC and physical layers as defined in IEEE standards. Due to the accuracy and its sophisticated graphical user interface, the OPNET modeller has been chosen for simulation.

The Zigbee model provided in OPNET 16 is suitable for modelling wireless sensor networks. Zigbee model suite in OPNET includes a discrete event simulation model, which allows the users to analyse the performance in Zigbee WPANs [6]. This includes a model of IEEE 802.15.4 MAC protocol. The designed system consists of three types of wireless sensor Zigbee nodes, a coordinator, a router and an end device (sensing node). [5]

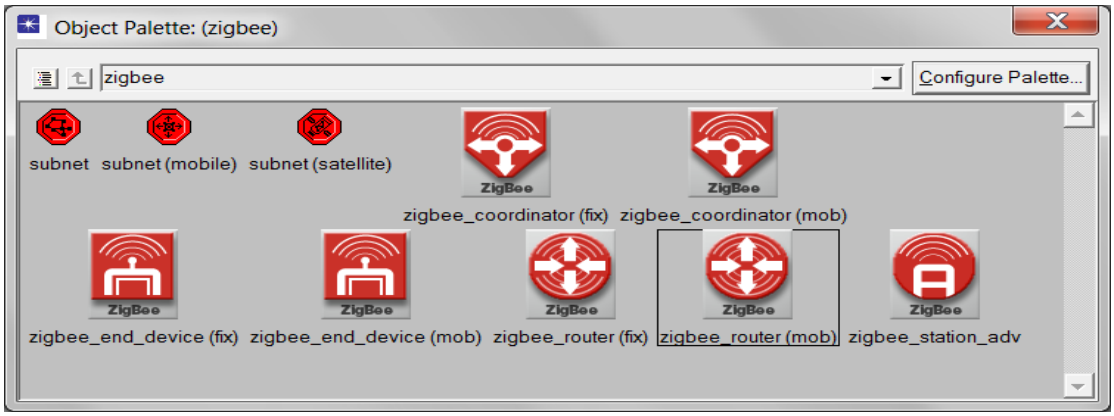

Fig 2. Zigbee object palette.

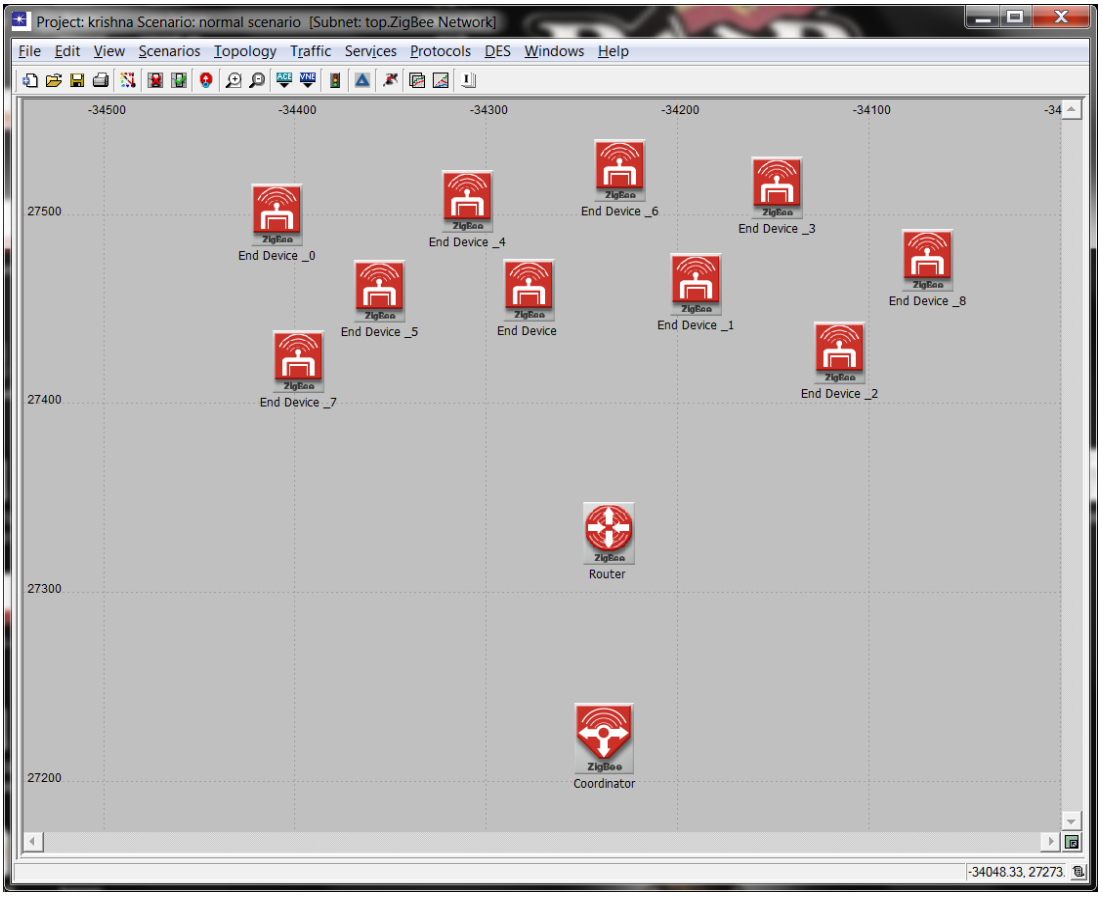

Figure 3: Main scenario of the experiment.

Zigbee coordinator: It forms the root of the network tree and might bridge the other networks. Most capable among the three type of Zigbee devices. There is only one Zigbee coordinator in each network as it is the device that started the network originally. It can store information about the network, including acting as the trust centre and repository for security keys.

Zigbee Router: It is a simple router that passes on the data from other devices. It keeps a routing table and controls allocation/de-allocation of local address for its allocated Zigbee end devices.

Zigbee End device: Contains just enough functionality to communicate with the parent nodes. It cannot route data from other devices. This allows the node to be asleep for a longer period of time and hence long battery life. [7]

When the simulation scenario of the study is considered, the objectives are:

a) The simulation model considered here has a tree topology where the communication takes place between the nodes coordinator, a router and the end device. Each of the operating devices has a unique address.
b) The traffic source generates the application data. This data can be generated either by the Personal Area Network coordinator or by the end device.
c) Each Zigbee node is powered with two AA batteries which should be sufficient for long interval of uninterrupted operation. Traffic by the attacker has been created using the traffic centre in OPNET modeller.
d) Different data rates and different types of data's are employed to represent a DoS attack. Various traffic parameters can be set as according to the requirement.
e) Every simulation scenario is considered to represent a typical attack and observe the consequences.
f) The simulation time is set to 10 hours for every run to make sure that the simulation reaches to steady state and average value converges.

VI. EVALUATION:

In order to evaluate the performance of the Wireless sensor networks, and to analyse the impact of the DoS attack, we need to measure the performance metrics of the network. The WSN is modelled by using Zigbee nodes in OPNET for analysis in details. Scenarios of DoS attack on the zigbee router, zigbee coordinator, and zigbee end device have been modelled with suitable parameters. Simulation results have been illustrated for performance measures such as throughput, and traffic sent in the nodes. The results are compared for various cases of DoS attacks and normal scenario. Figures are presented for critical evaluation of various attacking scenarios.

Our standard scenario for all the experiments contains the following parameters:

1. At first 10 Zigbee end device have been considered depending on the conditions set to obtain the desired results.
2. One Zigbee router is used as a router gateway, to connect the Zigbee coordinator and the end devices.
3. A Zigbee coordinator forms the root of the network tree and bridge with the other networks. It stores information about the network, including the acting trust centre and repository for security keys.
4. The traffic in the network can be set as per the requirements. Destination of the traffic is set to end device, via router. Packet size and interarrival times are varied accordingly.

Simulation results of Attack on router:

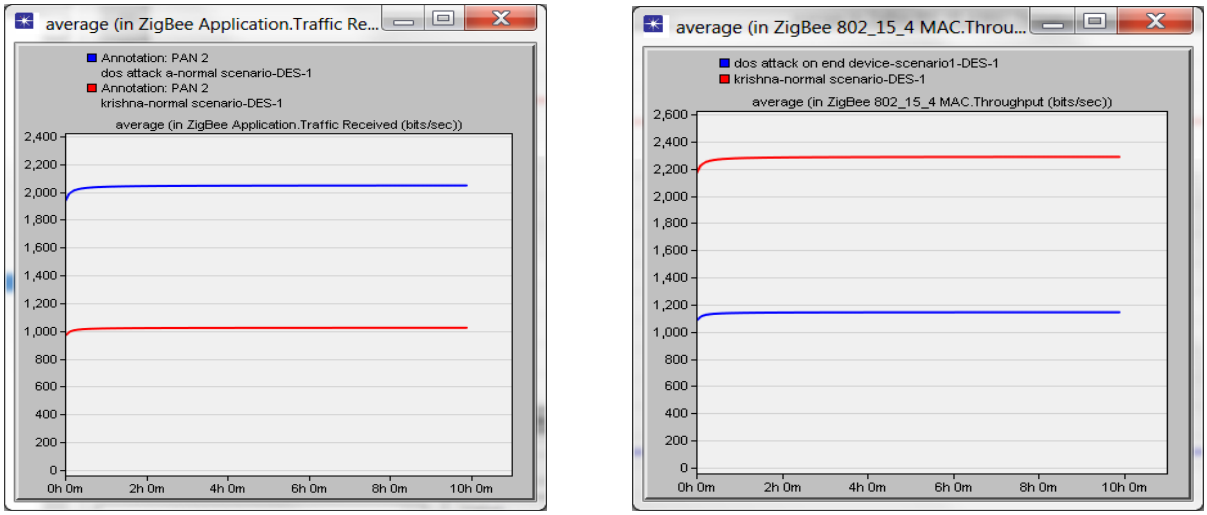

Figure 4: Average Traffic received and average throughput during Normal scenario and during DOS attack on router.

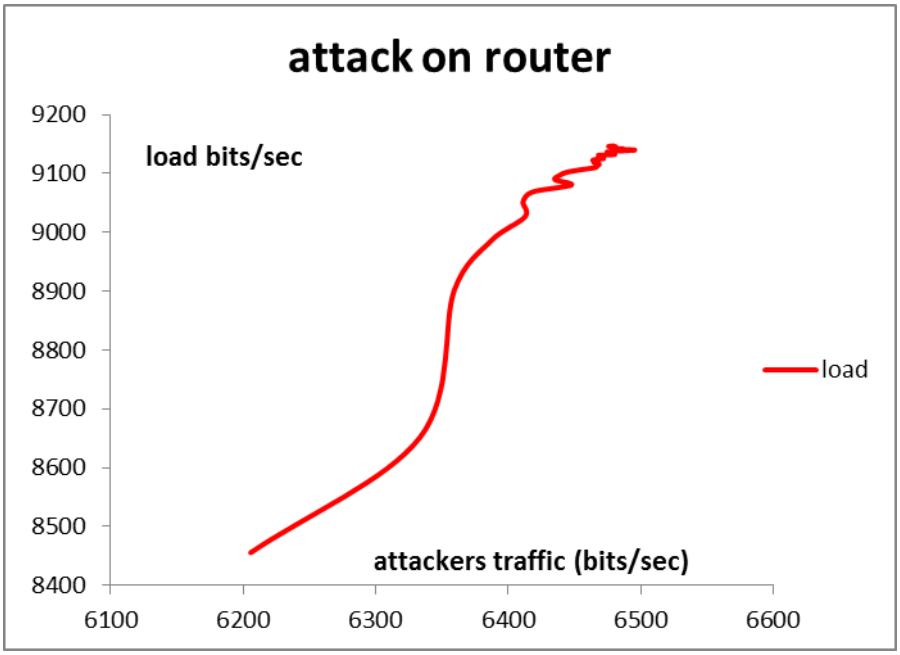

Figure 5: Average Load vs. Average Traffic of attacker during attack on router

In figure 5, the impact of the load on the network due to attacker's traffic is shown, while there is an attack on the router. The Denial of Service attack on the router, affects the performance of the overall network severely. The attack mainly degrades the performance due to the over load of traffic, as shown in the figure 5.

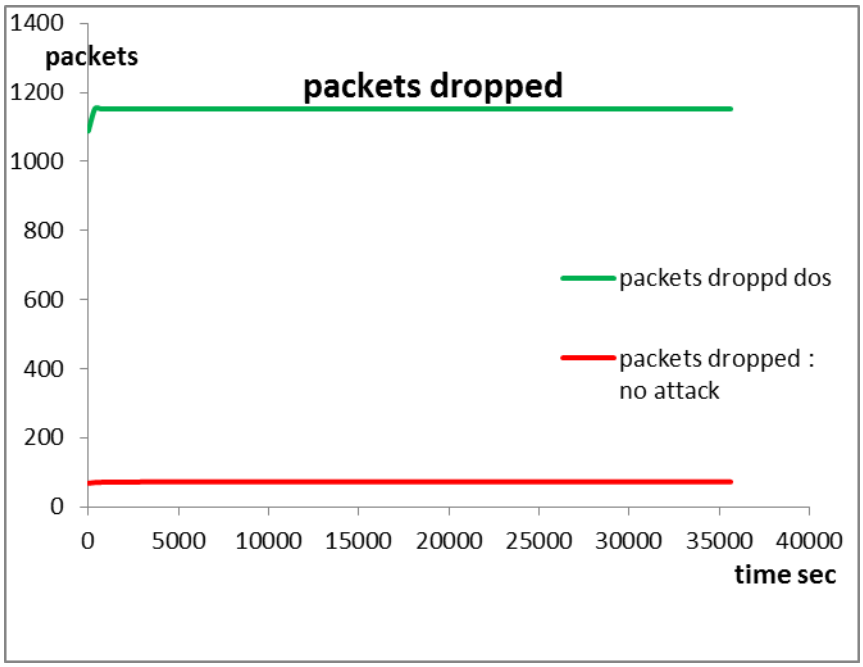

Figure 6: Average Packets dropped during no attack and DoS attack on router.

Figure 6, clearly shows that in a span of 10 hours, the number of packets dropped in DoS attack is nearly 1200 packets as compared to merely a 100 packets during the period with no attacks. This is a significant gap to evaluate the performance of the network in both the cases. The reason for the significant difference in loss of packets is the faulty traffic of the attacker which reduces the performance drastically and overloads the network. As the attacker overloads the network the legitimate users are not able to use the resources available.

In figure 7, the impact of load on the network due to traffic introduced by attacker is shown. This time the attack is on the coordinator. Due to the Denial of Service attack on the coordinator, there is a deep impact which degrades the performance significantly due to the over load of traffic, as shown in the graph. The load in case of attack on coordinator is higher i.e. (27500 bits/sec) compared to the load in case of an attack on router i.e. (9100 bits/sec) and attack on end device. Hence, the simulation results show that the impact of DoS attacks on performance of WSN can be more severe, if carried out on coordinator, instead of just targeting the router or end devices. In case of no attack, as shown in figure 8, the load on the network is much lower compared to all the other case of attacks.

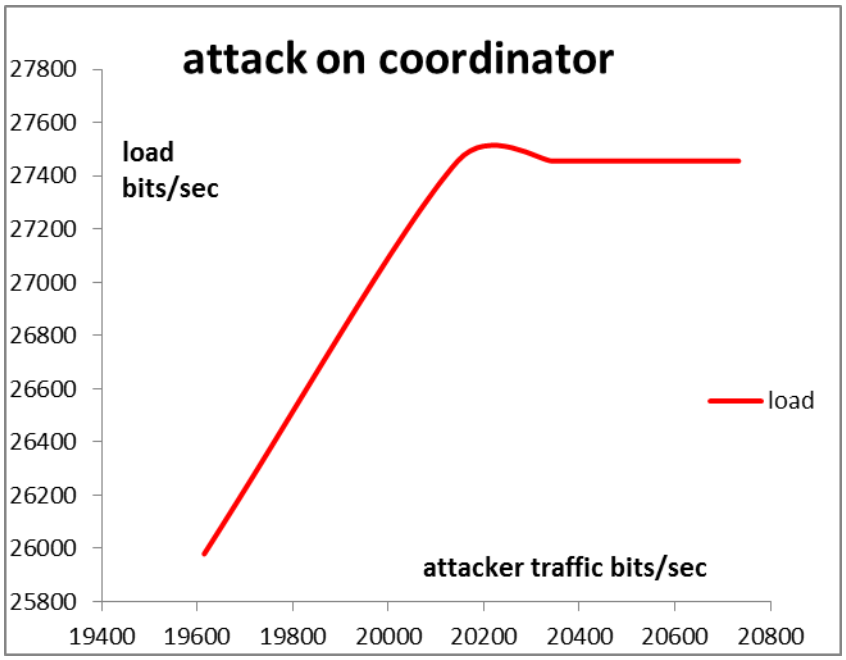

Figure 7: Average Load vs. Average Traffic of attacker during attack on coordinator

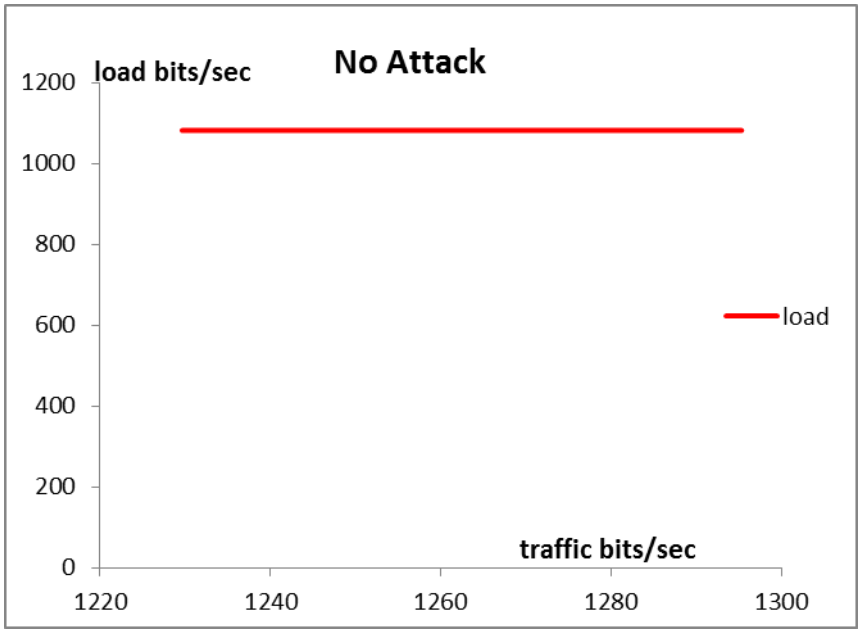

Figure 8: Average Load vs. Average Traffic of attacker in case of no attacks

VII. CONCLUSION:

This paper presented a simulation study of a Wireless Sensor Network to analyse the effects of various kind of attacks. The scenarios considered are no attack, attack on coordinator, attack on router and attack on the end devices. The simulation tool OPNET 16.0 is used effectively for detailed analysis. The scenarios considered are mainly taken from the literature. The simulation

results show that the impact of Denial of Service attacks on performance of WSN can become quite significant. In case there is an attack on the coordinator, node the performance degradation is more severe. This is mainly because the other nodes cannot access to relevant information used for routing which is available in the coordinator node. The effects of the DoS attack targeting the router node is also quite significant, but routing related computations can be conducted in coordinator node in case the gateway node is overwhelmed. In case of attacks on end devices the overall network is not affected as severely as the ones mentioned above.

It is desirable to further extend these studies in order to analyse the effects of DoS on energy related policies. Such a study would be essential since energy consumption is very critical for WSNs.

REFERENCES:

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. A survey on sensor networks, *IEEE Communications Magazine*, 40(8):102–114, August2002.

[2] Healy.M, Newe.T, Lewis.E, 'Security for Wireless Sensor Networks: A Review', IEEE Sensor Application Symposium, New Orleans, LA, USA-Feb 17-19, 2009.

[3] Raymond, D.R, Midkiff, S.F, 'Denial of Service in Wireless Networks: Attacks and Defences, IEEE CS: Security and Privacy, 2008,pg 74-81.

[4] Yahaya.F.H, Yussoff.Y.M, Rahman.R.Ab, Abidin.N.H,'Performance Analysis of Wireless Sensor Network', 5th International Colloquium on Signal Processing & its Applications (CSPA), 2009.

[5] Vlajic.N, Stevanovic.D, Spanogiannopoulos.G, 'Strategies for improving performance of IEEE 802.15.4/Zigbee WSNs with path constrained mobile sinks', Computer Communication Journals, 2010.

[6] OPNET Technologies, www.opnet.com

[7] ZigBee Specification v1.0: ZigBee Specification (2005), San Ramon,CA, USA: ZigBee Alliance http://www.zigbee.org/en/spec_download/download_request.asp

[8] Rui Silva, Serafim Nunes "Security Issues on ZigBee" (2005), http://rtcm.inescn.pt/fileadmin/rtcm/WorkShop_22_Jul_05/s2_Security Issues_on_ZigBee.pdf. accessed: 5 January 2009.